Práctica: Firmar digitalmente un mensaje

Objetivo: Realizar un hash de un mensaje y firmarlo con una clave privada, comprobar su veracidad cotejándola con la clave publica

Desarrollo:

1. Crear un clase para llevar a cabo la generación de clave, firma y comprobación
   1.1. Generador de claves

```
private static KeyPair generarClaves() throws Exception {
        KeyPairGenerator keyGen = KeyPairGenerator.getInstance("DSA");
        keyGen.initialize(1024);
        KeyPair ParClaves = keyGen.genKeyPair();
        return ParClaves;
}
```

   1.2. Firma de un mensaje

```
private byte[] firmar(PrivateKey clave, String str) throws Exception {

        byte[] cadenaByte = str.getBytes("UTF8");
        Signature sig = Signature.getInstance(clave.getAlgorithm());
        sig.initSign(clave);

        sig.update(cadenaByte, 0, cadenaByte.length);
        return sig.sign();
}
```

   1.3. Comprobación de la firma

```
private static Boolean comprobarFirma(PublicKey clave, String str,
        byte[] firma) throws Exception {
        byte[] cadenaByte = str.getBytes("UTF8");

        Signature sig = Signature.getInstance(clave.getAlgorithm());
        sig.initVerify(clave);
        sig.update(cadenaByte, 0, cadenaByte.length);

        if (sig.verify(firma))
                return true;
        else
                return false;
}
```

2. Firmar mensajes y comprobar su firma
3. Manipula el mensaje y vuelve a comprobar la firma

Web: www.sidertia.com
Email: info@sidertia.com
Tel: 646.366.781 | 646.116.305
Centro de Empresas Carabanchel
C/ Cidro, 3 - Oficina 207 28044 MADRID